

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kevin Corrigan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 2015. I am currently assigned to the Violent Crime Task Force of the Tampa Division of the FBI. During my time as a Special Agent with the FBI, I have participated in violent crime investigations as the primary investigator or in a subsidiary role. I am familiar with the procedures, activities, and investigative techniques associated with violent crime investigations, to include cases of online interstate threats and harassment, in violation of 18 U.S.C. §§ 875(c) and 2261A. Prior to working with the FBI, I served as a police officer in Charleston, South Carolina, and an Assistant State Attorney in Orlando, Florida.

2. This affidavit is being made in support of an application for the issuance of a search warrant for the residence of Evan Stauffer (“STAUFFER”) located at **10516 E. 40th Terrace, Kansas City, Missouri** (the “**TARGET RESIDENCE**”), which is more fully described in **Attachment A**. As set forth in more detail below, there is probable cause that the **TARGET RESIDENCE** contains evidence of violations of cyberstalking, in violation of 18 U.S.C. § 2261A(2)(b), interstate threats, in violation of 18 U.S.C. § 875(c), and making obscene and harassing telephone calls, in violation of 47 U.S.C. § 223(a)(1)(A), specifically information contained within

electronic media, computers, or devices such as smart phones, which constitute evidence or instrumentalities of those violations as described **Attachment B**.

3. I am requesting authority to search the **TARGET RESIDENCE**, which includes the physical structure, as well as any computer and computer media and electronic storage devices located therein. I also request to seize all items listed in Attachment B as instrumentalities, fruits, and/or evidence of criminal activity.

4. The facts contained in this affidavit are drawn from personal knowledge based on my participation in this investigation, information from other criminal investigators, information from law enforcement officers, information from agency reports, and the review of documents provided to me by witnesses and by law enforcement officers.

STATUTORY AUTHORITY

5. Title 18, United States Code, section 2261A(2)(B) prohibits a person from acting “with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress to a person.”

6. Title 18, United States Code, section 875(c) prohibits a person from “transmit[ing] in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.”

7. Title 47, United States Code, section 223(a) prohibits, among other things, a person from making or causing the telephone of another repeatedly or continuously to ring, with the intent to harass any person at the called number, and “making repeated telephone calls or repeatedly initiating communication with a telecommunications device, during which conversation or communication ensues, solely to harass any specific person.”

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

8. As described above and in Attachment B, this application seeks permission to search for records that might be found at the **TARGET RESIDENCE**, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

9. *Probable cause.* I submit that if a computer or storage medium is found at the **TARGET RESIDENCE**, there is probable cause to believe records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not

currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

10. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET RESIDENCE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively,

to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary

to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to engage in cyberstalking, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

11. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be

necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **TARGET RESIDENCE**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

PROBABLE CAUSE

Summary

13. For nearly two years, STAUFFER has engaged in a campaign of online and telephonic harassment and threats against Victim 1 and Victim 2, who reside in the Middle District of Florida. Beginning on an unknown date, but no later than in or around July 2020, and continuing to the present, STAUFFER engaged in a course of conduct with the intent to harass and intimidate the victims. Specifically, STAUFFER

cyberstalked, harassed, and threatened several victims through repeated emails, phone calls, text messages, and social media messages from numerous phone numbers and social media accounts, which were transmitted in and affected interstate commerce.

14. The Pasco County Sheriff's Office initiated the investigation and subsequently sought the assistance of the FBI after determining there were many victims located within the Middle District of Florida and STAUFFER was located in the Western District of Missouri.

Interview of Victim 1 and Victim 2

15. On or about December 6, 2022, the FBI interviewed Victim 1, an adult male, and Victim 2, his fiancé and cohabitant. Victim 1 and Victim 2 provided the information below:

16. In or around 2019, Victim 1 started chatting with an individual later identified as STAUFFER on the website fantasyfeeder.com. STAUFFER is an adult male but had identified himself to Victim 1 as a woman named "Jessica Riley". Victim 1 and STAUFFER chatted online for a few months about their shared fetish of overeating. Eventually, Victim 1, who thought STAUFFER was a woman, shared his Instagram account with STAUFFER and the conversations then shifted to Instagram messenger. STAUFFER utilized an Instagram account with the handle "Jessica Riley" and displayed photos of a young adult female. STAUFFER and Victim 1 spoke extensively via Instagram messenger, then later exchanged phone numbers. All the conversations between STAUFFER and Victim 1 were in text form (no verbal or video conversations had taken place up to this point).

17. In or around July 2021, Victim 1 attempted to end the online/text relationship with STAUFFER because Victim 1 wanted to have an exclusive relationship with his now fiancé, Victim 2. After Victim 1 informed STAUFFER that he no longer wished to continue their online relationship, STAUFFER told Victim 1 that if he ceased chatting with him, STAUFFER would tell Victim 1's then girlfriend (Victim 2) about his overeating fetish. Victim 1 felt blackmailed but still refused to continue chatting with STAUFFER.

18. For the next 18 months, Victim 1 and Victim 2 received an inordinate amount of phone calls (sometimes over a thousand calls per day), text messages, and social media messages from STAUFFER demanding that Victim 1 break up with Victim 2 and reestablish his relationship with STAUFFER. Almost all of the calls came from different phone numbers. STAUFFER also harassed dozens of people who knew Victim 1 by sending them screenshots of past embarrassing conversations between STAUFFER and Victim 1. STAUFFER accompanied those messages with false stories that Victim 1 drugged and raped STAUFFER and had repeatedly abused STAUFFER because he is transgender. Victim 1 has never met STAUFFER in person.

19. The harassment was so extensive that it significantly affected Victim 1 and Victim 2's personal lives and negatively affected Victim 2's business. Victim 1 estimated that over the past 18 months, close to 100 people have complained to Victim 1 and Victim 2 that they were being similarly harassed by STAUFFER's repeated communications where he made false allegations of rape and abuse by Victim 1 and Victim 2. These complainants included the victims' family members, neighbors,

clients, friends, and associates. Victim 2 told the FBI that STAUFFER found her business social media accounts and has been trying to destroy her business. Victim 2 indicated that STAUFFER created fake online client profiles and left negative public reviews about Victim 2's business. STAUFFER also created hundreds of fake "leads for work", which made it impossible for Victim 2 to decipher between real and fake potential clients. At least six of Victim 2's clients have been harassed by STAUFFER with messages indicating that Victim 2 enables a rapist, amongst other false allegations.

20. Victim 1 and Victim 2 told the FBI that they had received messages from STAUFFER indicating that the harassment will never stop, and that STAUFFER will continue to harass everyone in their lives until Victim 1 and Victim 2 end their relationship. Victim 1 and Victim 2 have received repeated threats of physical violence from STAUFFER, including photos of their home and vehicles, suggesting to the Victims that STAUFFER was watching them.

21. Victim 1 and Victim 2 have taken extensive steps to block STAUFFER from harassing them. They changed their phone numbers multiple times, restricted their social media access, and notified their associates, friends, and family of their cyberstalking problem. To date, Victim 1 and Victim 2 have spent hundreds of dollars on private investigators to help identify STAUFFER because after multiple complaints to local police, the harassment and threats only got worse.

22. After consulting with local police detectives, Victim 1 decided to attempt to cease the harassment by engaging in a conversation with STAUFFER. In or around

December 2021, Victim 1 invited STAUFFER to a video chat. Prior to this video chat, Victim 1 had never spoken to STAUFFER by any means other than text communication. STAUFFER agreed, and on or about December 29, 2021, Victim 1 recorded a video chat between STAUFFER and himself. In the video chat, STAUFFER admitted to repeatedly contacting Victim 1, Victim 2, and many of their associates. Victim 1 told the FBI that it was apparent during the video chat that he was speaking to a male presenting as a female. Victim 1 told the FBI that STAUFFER made the admission and told Victim 1 that STAUFFER would never do it again. After the video chat, however, the harassment increased exponentially; STAUFFER began calling Victim 1 and Victim 2 approximately 1,000 times per day.

23. Victim 1 told the FBI that he had discovered the true identity of STAUFFER in or around January 2022, when Victim 1 downloaded and utilized a cellphone application to unmask the caller ID of any person calling him. In or around January 2022, Victim 1 received a phone call from an individual using phone number 816-550-8510. According to the cellphone application, the caller ID associated with phone number 816-550-8510 was “Evan Stauffer.” Victim 1 and Victim 2 found the Facebook profile of Evan Stauffer and noticed that he was “friends with” the Facebook account of “Jessica Riley.” “Jessica Riley” was one of the Facebook accounts STAUFFER used to harass Victim 1. Victim 1 reviewed the profile photos displayed on the Facebook account of “Evan Stauffer” and believed the photos were of the same person he had video chatted with in or around December 2021.

24. An FBI agent showed Victim 1 the driver's license photo of STAUFFER and Victim 1 indicated that it was the same person Victim 1 had video chatted with in or around December 2021, except in the video chat, the person was wearing a wig and presenting as a female.

25. In or around December 2022, FBI agents received approximately 150 screenshots of conversations from the Pasco County Sheriff's Office ("PCSO") that Victim 1 and Victim 2 had previously provided to PCSO detectives. A review of the screenshots revealed the conversations were a mixture of text messages and social media conversations from unknown phone numbers to Victim 1, Victim 2, or their associates. According to the victims, the screenshots show messages they had received from STAUFFER, as well as messages that were forwarded to them by their friends, family, and associates who had also received the messages from STAUFFER. Below are a few examples of the screenshots:

From 715-303-2882 to Victim 2

"I swear to fucking God I'm never going to stop. I will continue to send you these messages until your guy's house goes on the market and you two are registered at different addresses. There is no reason on Earth why you two should still be together other than that fact that you are a fucking obese desperate BITCH! And if I ever see you two tagged in a picture again, I'll send these messages to all your friends and clients again, reminding them how fucking desperate you are to stay with that bastard. Your guy's "relationship" has almost killed me several times and I will not take it any more!!!! LEAVE HIM YOU DESPERATE HO!!!"

From 813-501-2434 to Victim 2

"Just sitting here watching your friends like a hawk, waiting for one of them to screw up and accidentally post a picture of you and [Victim 1] together. Then all hell will break loose and it will get REALLY nasty. I can promise you that."

From 813-543-5170 to Victim 2

“if you would just break up with him, I will leave you the fuck alone. I’ll even help you with your business and promote it if you want me to. The only thing I have against you is you’ve taken him away from me multiple times. But if you’ll walk away from him, you’ll be free of me. Right now, I don’t know if you guys are even still together for sure, but I assume you are, but because I don’t know for sure, I am leaving you friends and clients alone for now (except the ones who are also friends with him). But if I EVER see you guys in another photo together that will add fuel to the fire, and I have the names and numbers of all your friends and clients written down (some of whom I haven’t contacted before) and I will blow up their phones several times a day with the screenshots of him flirting with me, just like I do to you now. I quit my job so I have nothing but time on my hands. If he wants to treat me like a sex toy and only talk to me when it’s convenient for him then I’m coming to do everything I can to make his life as difficult as possible and yours if you stay with him.”

From 727-308-3535 to associate of the victims

“This week is going to be so much fun. [Victim 2], a person who makes women beautiful for a living, is engaged to a drug rapist. I strongly suggest you run from him as soon as possible before your reputation truly gets tarnished beyond repair because I’m not holding back the truth at all anymore.”

Between 813-815-4991 and associate of the victims

813-815-4991: “She knows about it but says it doesn’t count as cheating because I’m transgender...so I guess that makes me less human?”

Victim Associate: “I have no idea what is going on as I am not involved..I have no idea who you are..please don’t message me. #STOP”

Between 727-440-0637 and associate of the victims

727-440-0637: [Screenshot of past conversation with Victim 1]

Victim Associate: Will you stop harassing me

727-440-0637: Yes I will. When she leaves him.

Between 813-473-6422 and associate of the victims

813-473-6422: [Screenshot of past conversation with Victim 1]

Victim Associate: "I'm calling the police. Leave me alone never text me again. This is harassment please stop."

813-473-6422: I'll stop when he talks to me.

From 813-942-6953 to associate of the Victims

"Fuck [Victim 2], when she stops being a transphobic cunt and leaves her cheating fiancé, I'll leave you alone #transphobe #cheatingischeating"

26. In or around December 2022, FBI agents observed a video that Victim 1 provided to the PCSO in or around February 2022. Victim 1 and Victim 2 told PCSO detectives and the FBI that the video was the aforementioned recording Victim 1 made of himself video chatting with STAUFFER in or around December 2021. In the video, FBI agents observed Victim 1 video chatting with an unknown subject. The unknown subject appeared to be a female with long hair that spoke in a masculine voice. When Victim 1 asked the subject why she contacted everyone, the subject replied, "I lost control of myself." Victim 1 begged the subject to stop contacting Victim 2 and leave her out of it. The subject stated that she was "really hurt and wasn't thinking." The subject also stated, "it wasn't 18 months straight. I took breaks and stopped. It was a cycle." When asked if she meant to reach out to all of those people, the subject stated, "I was so sad...I had nothing to lose because you already hated me...I was so unhappy and miserable." The subject later said that she was "sorry" and "she would never do it again." The unknown subject spoke with a distinct and obvious lisp.

27. FBI agents spoke with a PCSO detective in or around December 2022. The detective informed the FBI that they had reviewed Victim 1's cellphone in or

around February of 2022 and observed that Victim 1 had received the following text messages:

January 8, 2022, from 316-600-3828

You are a fucking idiot. You would seriously rather me blow up your phone and everyone you knows phone than talk to me???? I'm never going to give up

January 5, 2022, from 813-596-0688

"I'm sending someone over to your house to beat the fucking shit out of you fucking retarded bastard I know where you live!! You'll be in the hospital very soon"

January 5, 2022, from 813-219-4972

"So I heard you are going to make a new Facebook account? Don't worry, I'll find it. Unless you use a different name and someone else's pictures. Same goes for your fat ho. Change your number? I'll find that too. I have my ways and you know it. You can run but you can't hide. I'm watching both of you like a hawk. You already knew hose I was after everything that went down this past year and a half and you decided to fuck with my head even more"

January 3, 2022, from 813-219-4972

"I already did. We video chatted and everything. This can go on for another 30 years. Trust me, I'll never let this go"

December 25, 2021, from 813-344-0629

"Ignoring me is a very bad idea. I'll literally blow your phone up until you fucking talk to me."

28. PCSO detectives served a subpoena upon Verizon Wireless and obtained call detail records with subscriber data associated with call number 816-550-8510, which was the phone number Victim 1 "unmasked" using the caller ID application on his cellphone. The FBI reviewed the records and observed that call number 816-550-8510 was subscribed to "Evan Stauffer" of Independence, Missouri. Additionally, FBI

agents observed that the call records show over 1,000 calls to *67[Victim 2's phone number] between the dates of January 10, 2022, and January 12, 2022.

29. PCSO detectives served a subpoena upon Text Plus, an internet service provider. FBI agents reviewed records received from Text Plus. The records show that the email estauffer99@gmail.com is the subscriber email associated with Text Plus call number 813-344-0629. This phone number (813-344-0629) is the same number that sent Victim 1 a threatening message on or about December 25, 2021. (See paragraph 27). The records, however, did not include a name or address associated with the account.

30. PCSO detectives served a subpoena upon Google LLC for subscriber information associated with estauffer99@gmail.com. FBI agents reviewed records received from Google LLC. The records indicate that the email address estauffer99@gmail.com is subscribed to "Evan Stauffer" of Independence, Missouri, with a subscriber phone number of 816-550-8510. This phone number is the same aforementioned Verizon phone number that called Victim 2 over 1,000 times in two days. (See paragraph 28).

31. On or about December 15, 2022, FBI agents received an audio recording of a phone call between Witness 1 and STAUFFER. Witness 1 is a private investigator who was hired by Victim 1 to locate STAUFFER. Witness 1 called STAUFFER under the guise of a delivery service attempting to deliver a package to STAUFFER. STAUFFER answered the call and confirmed that he is "Evan Stauffer". After listening to the recording, FBI agents observed that STAUFFER spoke with the same

distinct and obvious lisp as the unknown subject in the recorded video chat with Victim 1. (See paragraph 22). The voice in both the recorded phone call and the recorded video chat appears to be of the same person.

32. In or around December 2022, STAUFFER threatened to blackmail Victim 2 if she did not provide STAUFFER with Victim 1's new phone number. In response, Victim 2 provided STAUFFER with Victim 1's phone number as well as the phone number of an FBI agent.

33. On or about December 19, 2022, an FBI agent received a phone call from call number 505-533-0637. The caller identified herself as "Samantha" and stated that she thought she was calling Victim 1's work phone number. The caller stated that she had received the [agent's] phone number from Victim 2. The voice sounded identical to the voice on the aforementioned recorded phone call and in the recorded video chat—there was a distinct and noticeable lisp. The caller stated that she was born a male but now identified as a woman and refused to provide her birth identity. The caller hung up once she realized she was not chatting with Victim 1, but immediately started sending the FBI agent text messages. In the text messages to the FBI agent, the caller admitted to sending threatening messages to Victim 1 because she "was pissed off." When asked about threats to Victim 2, she stated, "I didn't threaten her. Not physically I threatened to ruin her reputation by spreading nothing but the honest to God truth about her." She also stated that Victim 2 was a "fucking transphobic whore. She totally deserves it."

34. As a result of STAUFFER's course of conduct, the victims viewed the messages as true threats and suffered substantial emotional distress.

35. Based on the facts presented in this affidavit, there is probable cause to believe that STAUFFER used electronic communication services (to include Verizon Wireless, Text Plus, Instagram, and Facebook) to repeatedly communicate with Victim 1, Victim 2, and their associates, with the intent to harass and intimidate Victim 1 and Victim 2. STAUFFER's conduct caused substantial emotional distress to Victim 1 and Victim 2. Additionally, on or about January 5, 2022, STAUFFER knowingly sent text messages using wireless communication services to Victim 1 containing a true threat to injure Victim 1 with the intent to communicate the true threat.

36. On December 23, 2022, the FBI obtained a federal complaint in the Middle District of Florida, case no. 8:22-mj-2241-MRM. The complaint charged STAUFFER with violations of cyberstalking, in violation of 18 U.S.C. § 2261A(2)(b), interstate threats, in violation of 18 U.S.C. § 875(c), and making obscene and harassing telephone calls, in violation of 47 U.S.C. § 223(a)(1)(A).

Identifying the TARGET RESIDENCE

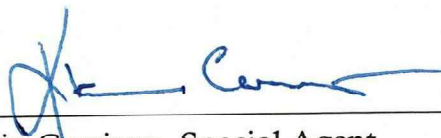
37. On or about December 28, 2022, FBI agents reviewed public utility records associated with the **TARGET RESIDENCE**. The records indicate that STAUFFER is the listed customer for the **TARGET RESIDENCE** and that payments have been made on the account every month starting in or around March 2022 and as recent as December 2022.

38. On or about December 28, 2022, the owner of the **TARGET RESIDENCE** told FBI agents that he rents the **TARGET RESIDENCE** to STAUFFER. The owner indicated that STAUFFER is the only resident at **TARGET RESIDENCE** and that he had lived there for an extended period of time.

39. On or about December 26, 2022, FBI agents spoke with a witness who lived near the **TARGET RESIDENCE**. The witness indicated that he/she observed STAUFFER exit the **TARGET RESIDENCE** on or about December 26, 2022, to walk his dog.

CONCLUSION

40. Based on the above information, probable cause exists that the **TARGET RESIDENCE**, as fully described in **Attachment A**, contains evidence, fruits, and/or instrumentalities of violations of cyberstalking, in violation of 18 U.S.C. § 2261A(2)(b), interstate threats, in violation of 18 U.S.C. § 875(c), and making obscene and harassing telephone calls, in violation of 47 U.S.C. § 223(a)(1)(A). Accordingly, I respectfully request a warrant to search the **TARGET RESIDENCE** and seize the items listed in **Attachment B**.



Kevin Corrigan, Special Agent
Federal Bureau of Investigation

Sworn to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 and 41(d)(3) via telephone this 3rd day of January, 2023.



HONORABLE W. BRIAN GADDY
United States Magistrate Judge
Western District of Missouri

By telephone at 4:30 pm

